

OGŁOSZENIE O DIALOGU TECHNICZNYM

I. ZAMAWIAJĄCY

Mazowiecki Urząd Wojewódzki w Warszawie

pl. Bankowy 3/5

00-950 Warszawa

II. DANE KONTAKTOWE ZAMAWIAJĄCEGO

Mazowiecki Urząd Wojewódzki w Warszawie

pl. Bankowy 3/5

00-950 Warszawa

Osoba wyznaczona do kontaktu:

p. Łukasz Dmowski – kierownik Oddziału Zamówień Publicznych

tel. 0 22 695 66 85

adres email: ldmowski@mazowieckie.pl

Wszelką korespondencję kierowaną do Zamawiającego należy opatrzyć dopiskiem: *„Dialog techniczny związany z postępowaniem o udzielenie zamówienia publicznego na zaprojektowanie i wykonanie Zintegrowanego Systemu Bezpieczeństwa w budynkach Mazowieckiego Urzędu Wojewódzkiego przy pl. Bankowym 3/5 i Al. Solidarności 81”*.

III. PODSTAWA PRAWNA

Dialog techniczny prowadzony jest na podstawie art. 31a - 31c ustawy z dnia 29 stycznia 2004 Prawo zamówień publicznych (Dz. U. z 2018, poz. 1986 z późn. zm.) oraz zgodnie z *„Regulaminem przeprowadzania dialogu technicznego”* opublikowanym na stronie internetowej Zamawiającego.

IV. PRZEDMIOT ZAMÓWIENIA ORAZ CEL PROWADZENIA DIALOGU

1. Zamawiający ogłasza dialog techniczny związany z postępowaniem o udzielenie zamówienia publicznego, którego przedmiotem jest na zaprojektowanie i wykonanie Zintegrowanego Systemu Bezpieczeństwa w budynkach Mazowieckiego Urzędu Wojewódzkiego przy pl. Bankowym 3/5 i Al. Solidarności 81.

Prowadzony Dialog Techniczny służyć będzie pozyskaniu informacji związanych z najnowszymi rozwiązaniami technicznymi, organizacyjnymi i technologicznymi dotyczącymi wdrożenia Zintegrowanego Systemu Bezpieczeństwa, który będzie pełnił funkcję:

- Systemu Kontroli Dostępu (SKD);
- Systemu Kontroli Ruchu Pojazdów;
- Systemu Depozytorów Kluczy;
- Systemu CCTV – rozbudowa i integracja istniejącego systemu (IP CCTV);
- Systemu monitoringu stanu zamknięcia/otwarcia drzwi zewnętrznych;
- Systemu sygnalizacji włamania i napadu (SSWiN) w wybranych lokalizacjach obiektu – rozbudowa, integracja bądź wymiana istniejących systemów lokalnych;

oraz będzie współpracował z istniejącym systemem sygnalizacji alarmu pożaru SAP (w tym z systemem wizualizacji) i będzie miał możliwość rozbudowy o system rejestracji czasu pracy pracowników MUW i ewentualne inne moduły (możliwe propozycje wykonawcy).

Zamawiający dopuszcza możliwość integracji i rozbudowy istniejących systemów bądź w przypadku braku takiej możliwości (nie dotyczy systemu SAP wraz z wizualizacją), realizacji systemu zamiennego.

Założenia Zintegrowanego Systemu Bezpieczeństwa MUW zawiera załącznik nr 3 do Ogłoszenia.

V. ZASADY PROWADZENIA DIALOGU

1. Dialog techniczny prowadzony będzie zgodnie z postanowieniami „Regulaminu przeprowadzania dialogu technicznego” opublikowanego na stronie internetowej Zamawiającego.
2. Warunkiem udziału w dialogu technicznym jest złożenie wniosku o dopuszczenie do udziału w dialogu, stanowiącego Załącznik nr 1 do niniejszego Ogłoszenia w terminie określonym w niniejszym Ogłoszeniu. Do wniosku Uczestnik obowiązany jest załączyć:
 - 1) dokument poświadczający należyte umocowanie do reprezentacji Uczestnika,
 - 2) wykaz wykonanych usług (wg wzoru stanowiącego załącznik nr 2 do niniejszego Ogłoszenia) wraz z dokumentami potwierdzającymi należyte wykonanie usług wymienionych w wykazie.
3. Zgodnie z treścią §5 ust. 7 „Regulaminu przeprowadzania dialogu technicznego”, Zamawiający informuje, iż o dopuszczenie do udziału w Dialogu mogą ubiegać się wyłącznie Uczestnicy, którzy wykażą, iż w okresie ostatnich 3 lat przed upływem terminu składania wniosków do dopuszczenia do udziału w Dialogu Technicznym (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie), zrealizował lub realizuje (przy czym w tym przypadku będzie liczona wartość zrealizowanej części przedmiotu umowy) co najmniej dwie usługi, z których każda polegała na

wdrożeniu systemu bezpieczeństwa, tj. obejmującego przede wszystkim system kontroli dostępu, o wartości minimum 200 000,00 zł (słownie: dwieście tysięcy złotych) brutto każda, w budynkach o powierzchni nie mniejszej niż 10 000 m² każdy. W przypadku usług realizowanych, wykonawca wykaże, że wartość zrealizowanej części usługi była nie niższa niż 200.000,00 zł brutto.

Na potwierdzenie spełniania ww. warunku Uczestnik złoży, wraz z wnioskiem o dopuszczenie do udziału w dialogu, wykaz wykonanych usług wraz z dokumentami potwierdzającymi należyte wykonanie usług wymienionych w wykazie (wg wzoru stanowiącego załącznik nr 2). Dokumenty potwierdzające należyte wykonanie usług wymienionych w wykazie należy dostarczyć zamawiającemu w oryginale lub kopii potwierdzonej za zgodność przez Uczestnika.

4. Dialog techniczny prowadzony będzie w języku polskim i ma charakter jawny, z zastrzeżeniem §6 ust. 10 „*Regulaminu przeprowadzania dialogu technicznego*”. Do dokumentów sporządzonych w innych językach niż polski muszą być dołączone tłumaczenia na język polski. Zamawiający nie wymaga tłumaczenia przysięgłego.
5. Dialog techniczny prowadzony będzie w formie indywidualnych spotkań lub grupowych z Uczestnikami. Zamawiający dopuszcza również możliwość wymiany korespondencji w postaci pisemnej lub elektronicznej
6. Termin zakończenia dialogu technicznego przewidywany jest na **31 lipca 2019**

VI. ZGŁOSZENIE DO UDZIAŁU W DIALOGU TECHNICZNYM

1. Podmioty zainteresowane udziałem w dialogu technicznym, spełniające wymagania określone w niniejszym Ogłoszeniu oraz w „*Regulaminie przeprowadzania dialogu technicznego*” składają prawidłowo wypełnione i podpisane wnioski o dopuszczenie do udziału w Dialogu technicznym (zgodnie ze wzorem stanowiącym załącznik nr 1) wraz z pozostałymi dokumentami wskazanymi w niniejszym Ogłoszeniu.
2. Wnioski o dopuszczenie do udziału w dialogu technicznym składa się w formie pisemnej.
3. Wnioski o dopuszczenie do udziału w dialogu technicznym należy przesać pocztą lub złożyć w sekretariacie w siedzibie Zamawiającego w Warszawie przy pl. Bankowym 3/5, Sekretariat Biura Obsługi Urzędu, pok. 52.
4. Termin składania wniosków o dopuszczenie do udziału w dialogu technicznym: **24 czerwca 2019.** Decyduje data wpływu do Zamawiającego.
5. Zamawiający nie jest zobowiązany dopuścić do dialogu technicznego podmioty, które złożą zgłoszenie do udziału w dialogu po wyznaczonym terminie.

Wniosek o dopuszczenie do udziału w Dialogu Technicznym

Ja niżej podpisany/My niżej podpisani

.....
.....
.....,

będąc upoważnionym/i/ do reprezentowania Uczestnika:

.....
.....
.....

nr telefonu; e-mail:

w odpowiedzi na publiczne ogłoszenie o dialogu technicznym nr BOU-IV.272.27.2019, składam niniejszy wniosek do dopuszczenie do dialogu technicznego, organizowanego przez Mazowiecki Urząd Wojewódzki w Warszawie, którego przedmiotem jest zaprojektowanie i wykonanie Zintegrowanego Systemu Bezpieczeństwa w budynkach Mazowieckiego Urzędu Wojewódzkiego przy pl. Bankowym 3/5 i Al. Solidarności 81.

Dane osoby upoważnionej przez Uczestnika do kontaktów:

Imię i nazwisko

Funkcja

e-mail:

tel.

W związku z wnioskiem do dopuszczenie do udziału w Dialogu Technicznym oświadczam, iż:

- 1) jestem należycie umocowany/a do reprezentowania Uczestnika na dowód czego przedkładam dokument potwierdzający moje umocowanie;
- 2) zapoznałem się z Regulaminem Przeprowadzania Dialogu Technicznego i w całości akceptuję jego postanowienia;

- 3) wyrażam zgodę na przetwarzanie i przechowywanie przez Mazowiecki Urząd Wojewódzki w Warszawie informacji zawartych w niniejszym Zgłoszeniu dla celów Dialogu lub Postępowania;
- 4) udzielam bezwarunkowej i nieograniczonej w czasie zgody na wykorzystanie informacji przekazywanych w toku Dialogu, w tym również informacji stanowiących przedmiot praw autorskich Uczestnika, na potrzeby przeprowadzenia Postępowania, którego przedmiotem jest zaprojektowanie i wykonanie Zintegrowanego Systemu Bezpieczeństwa w budynkach Mazowieckiego Urzędu Wojewódzkiego przy pl. Bankowym 3/5 i Al. Solidarności 81, w tym w szczególności do przygotowania opisu przedmiotu Zamówienia, specyfikacji istotnych warunków Zamówienia lub określenia warunków umowy dla Zamówienia, z zastrzeżeniem § 6 ust. 10 Regulaminu Przeprowadzania Dialogu Technicznego;
- 5) wyrażam zgodę na rejestrowanie przez Zamawiającego przebiegu Dialogu, za pomocą środków technicznych rejestrujących dźwięk i obraz;
- 6) wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO¹ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udział w niniejszym dialogu².

Załącznikami do niniejszego wniosku, stanowiącymi jego integralną część są:

- 1)
- 2)
- 3)

....., dn.2019 r.

.....
(podpis/y osoby/osób uprawnionej/ych)

¹ rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)

² w przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Wykaz wykonanych usług

Nazwa (firma) i adres odbiorcy	Szczegółowy opis wykonanych usług	Wartość brutto wykonanej usługi lub części usługi	Data wykonania usługi

Uwaga! Opis wykonanych usług musi zawierać informacje pozwalające jednoznacznie stwierdzić, że Uczestnik spełnia warunek udziału w dialogu technicznym, o którym mowa w rozdziale V p. 2 ogłoszenia o dialogu technicznym.

Do powyższego wykazu załączam/załączamy dowody potwierdzające, że usługi, o których mowa wyżej, zostały wykonane należycie lub są wykonywane należycie.

- 1)
- 2)
- 3)

....., dn.2019r.

.....
(podpis/y osoby/osób uprawnionej/ych)

Założenia Zintegrowanego Systemu Bezpieczeństwa MUW

- 1) ZSB MUW, będzie realizować następujące funkcje:
 - Systemu Kontroli Dostępu (SKD);
 - Systemu Kontroli Ruchu Pojazdów;
 - Systemu Depozytorów Kluczy;
 - Systemu CCTV – rozbudowa i integracja istniejącego systemu (IP CCTV);
 - Systemu monitoringu stanu zamknięcia/otwarcia drzwi zewnętrznych;
 - Systemu sygnalizacji włamania i napadu (SSWiN) w wybranych lokalizacjach obiektu – rozbudowa, integracja bądź wymiana istniejących systemów lokalnych;
- 2) ZSB będzie współpracował z istniejącym systemem sygnalizacji alarmu pożaru SAP (w tym z systemem wizualizacji).
- 3) ZSB powinien mieć możliwość rozbudowy o system rejestracji czasu pracy pracowników MUW;
- 4) W przypadku braku możliwości integracji obecnie funkcjonujących systemów (nie dotyczy systemu SAP wraz z wizualizacją), należy zaproponować systemy zamienne.

Wymagania w zakresie możliwości Systemu i aplikacji obsługującej System

- 1) Aplikacja ZSB ma cechować się otwartą architekturą tj. podatnością na rozszerzenia, możliwością rozbudowy systemu zarówno pod względem sprzętowym, jak i oprogramowania;
- 2) Aplikacja musi obligatoryjnie wykorzystywać interfejs w języku polskim;
- 3) Aplikacja musi wykorzystywać sprawdzone rozwiązania dla obiektów dużych i rozproszonych (porównywalnych wielkością do MUW);
- 4) Aplikacja ma zapewniać integrację i nadzór w czasie rzeczywistym informacji o stanie bezpieczeństwa obiektów, ich analizę i wspomaganie w podejmowaniu decyzji, w zależności od rodzaju wykrytych zagrożeń;
- 5) Aplikacja ma zapewniać centralne zarządzanie każdym z podłączonych do niego urządzeń np. konfigurowanie parametrów pracy, modyfikację uprawnień dostępu, aktualizację oprogramowania, itd. zgromadzone dane z pracy całego systemu służą do tworzenia różnorodnych raportów, wykorzystywanych przez specjalistyczne komórki danej organizacji.
- 6) Aplikacja powinna zapewniać dostęp do zintegrowanego systemu bezpieczeństwa MUW również z poziomu przeglądarek internetowych;
- 7) Aplikacja musi posiadać mechanizmy zabezpieczające przed nieuprawnionym dostępem z zewnątrz (kompatybilne z systemem posiadanym przez Zamawiającego);
- 8) Aplikacja musi być dostępna poprzez sieć LAN (intranet);
- 9) Aplikacja musi zapewniać monitorowanie i zarządzanie sygnałami z podsystemu sygnalizacji włamania i napadu, może wykorzystywać istniejące struktury sieci LAN do zapewnienia pełnej integracji obiektowych systemów zabezpieczeń, takich jak: system CCTV, SSWIN, SKD, sygnalizacji pożaru (system wizualizacji);
- 10) Aplikacja powinna zapewniać zdalne zarządzanie strefami ochrony (wył/zał. zależne lub niezależne) – według 6 scenariuszy (I stan normalny, II – ewakuacja, III – Alfa, IV – Brawo, V – Charlie, VI – Delta);
- 11) Aplikacja zapewni obsługę kontroli pracy firm realizujących usługi ochrony na podstawie generowanych raportów (system patrolowania);
- 12) Aplikacja zapewni wizualizację stanów alarmowych;
- 13) Aplikacja musi zapewniać dostęp do danych systemu poprzez sieć LAN – MUW oprogramowanie winno umożliwiać monitorowanie przejść on-line - kontrolę czytników kart elektronicznych sprzężonych z zamkami otwierającymi drzwi, predefiniowanie reguł dostępu poszczególnych pracowników do stref chronionych;
- 14) Aplikacja powinna analizować istotne z punktu widzenia użytkownika informacje, zapewniać ich podgląd i wydruk. W szczególności powinna umożliwiać sprawdzenie, kto i kiedy otwierał dane przejście.

- 15) Należy zaplanować stanowisko wydawania przepustek (wejście C + dodatkowe / okazjonalne w wejściu B). Stanowisko takie ma służyć edycji przepustek oraz może spełniać funkcje wizualizacji stanu systemu (wizualizacja nie dotyczy wejścia B).
- 16) Projektant uwzględni także kwestie wdrażania nowych kart oraz nadawanie i odbieranie stałych uprawnień dla pracowników.

Wymagania w zakresie systemu kontroli dostępu (SKD)

- 1) Należy przewidzieć obustronną kontrolę dostępu w następujących lokalizacjach:
 - drzwi zewnętrzne wejście A (dziejnec od ul. Elektoralnej);
 - drzwi zewnętrzne w przejściu pomiędzy dziedzińcem głównym a dziedzińcem od ul. Elektoralnej - 2 szt.;
 - drzwi zewnętrzne w bramie dziedzińca głównego (klatka schodowa K9);
 - drzwi zewnętrzne wejście E tj. klatka schodowa K14 oraz wejście na klatkę schodową K10 (od pl. Bankowego);
 - furtka w bramie wjazdowej od ul. Solidarności;
 - bramki w wejściu B (2 szt.);
 - bramki w wejściu C (5 szt.);
 - bramka w wejściu D (1 lub 2 szt.) – w danej lokalizacji istnieje bramka kontroli dostępu, w przypadku braku możliwości włączenia urządzenia do systemu, bądź braku możliwości instalacji urządzenia o zbliżonych parametrach wizualnych należy przewidzieć wymianę urządzenia;
 - drzwi ppoż na I piętrze (wygrodenie klatek schodowych K7 i K9 od strony korytarza VIP)
 - włączenie do systemu SKD systemu obecnie funkcjonującego w Punkcie Obsługi Klienta MUW zlokalizowanym w wejściu F (ul. Solidarności)
- 2) Należy przewidzieć w holu budynku B w wejściu C „punkt recepcyjny” zapewniający kontakt z klientami i wydawanie „kart gościa” (nie dotyczy aranżacji recepcji). Założeniem jest, aby klienci wchodzili wejściem C, a doraźnie istniała możliwość, w przypadku organizacji uroczystości objętych systemem zaproszeń, uruchomienia wejścia B;
- 3) Należy przewidzieć, aby wejścia zewnętrzne (poza wejściem C) były wejściami dostępnymi wyłącznie dla pracowników z elastyczną możliwością tworzenia uprawnień dostępu do poszczególnych przejść;
- 4) Należy uwzględnić dla SKD możliwość przydzielania czasowego dostępu do wybranych stref w obiekcie;
- 5) SKD musi współpracować z istniejącymi lokalnymi systemami kontroli dostępu (pomieszczenia Punktu Obsługi Klienta, Biuro Ochrony, WBZK, Serwerownie, pomieszczenia socjalne, itd.) w tym celu należy uwzględnić aby System obsługiwał karty dostępu ujednolicone dla wszystkich lokalizacji;
- 6) Karty SKD powinny obsługiwać również podsystem parkingowy oraz podsystem elektronicznych depozytorów kluczy;
- 7) SKD musi być administrowane poprzez aplikację, gwarantując efektywny mechanizm przydzielania i migracji uprawnień w zależności od przydzielonej roli użytkownika;
- 8) SKD ma mieć możliwość rozbudowy o funkcję rejestracji czasu pracy;
- 9) Przy każdym przejściu należy zaprojektować urządzenia umożliwiające otwarcie w sytuacji awaryjnej (np. pożaru);
- 10) Wskazane przez Zamawiającego strefy objęte SKD powinny mieć możliwość dualnego lub alternatywnego do karty potwierdzenia identyfikacji (np. pom. socjalne);

Wymagania w zakresie Systemu Kontroli Ruchu Pojazdów (rozpoznawanie nr rejestracyjnych)

- 1) Należy przewidzieć integrację istniejącego systemu (dotyczy wjazdu na dziedziniec główny oraz wjazdu na dziedziniec od ul. Elektoralnej);
- 2) Należy przewidzieć rozbudowę istniejącego systemu (dotyczy wjazdu na dziedziniec od al. Solidarności);
- 3) System Kontroli Ruchu Pojazdów powinien zapewniać otwieranie szlabanów przy użyciu obecnie funkcjonującego systemu rozpoznawania tablic rejestracyjnych, a także otwieranie przez pracownika ochrony w portierni w wejściach C i F (oraz w pomieszczeniu ochrony wskazanym przez Zamawiającego) z zapewnieniem kontaktu głosowego i podglądu CCTV z gościem wjeżdżającym na parking oraz ewentualne rozwiązanie w oparciu o karty magnetyczne/pilot,

Wymagania w zakresie depozytorów kluczy

- 1) Należy przewidzieć budowę systemu elektronicznych depozytorów kluczy z zachowaniem zasady jednej karty;
- 2) Depozytory w budynku MUW powinny być rozmieszczone w lokalizacjach wskazanych przez Zamawiającego i w ilości zapewniającej właściwe funkcjonowanie obiektu;

Wymagania w zakresie współpracy z istniejącym systemem IP CCTV

- 1) Wymagane jest zaplanowanie niezbędnego zakresu rozbudowy Systemu IP CCTV ze względu na potrzeby Zintegrowanego Systemu Bezpieczeństwa;
- 2) Zamawiający oczekuje uwzględnienia współdziałania systemu CCTV z integrowanymi podsystemami ochrony: np. dowiązania do zdarzeń alarmowych, weryfikacja alarmów pożarowych, wsparcie weryfikacji użytkowników SSWiN i SKD, itd.;

Wymagania w zakresie systemu monitoringu stanu zamknięcia/otwarcia drzwi

- 1) Należy przewidzieć system monitoringu stanu zamknięcia drzwi zewnętrznych, w taki sposób aby wizualizacja systemu SAP (w portierni wejście C oraz pomieszczenie ochrony) sygnalizowała stan zamknięcia poszczególnych drzwi (na wizualizacji oraz dźwiękowo).
- 2) Należy przewidzieć system monitoringu stanu zamknięcia drzwi ppoż na I piętrze (wygrodenie klatek schodowych K7 i K9 od strony korytarza VIP), w taki sposób aby wizualizacja systemu SAP (w portierni wejście C oraz pomieszczenie ochrony) sygnalizowała stan ich (na wizualizacji).

Wymagania w zakresie SSWiN

- 1) Należy przewidzieć integrację istniejących systemów WiN);
- 2) Należy przewidzieć możliwość przyjmowania informacji z wydzielonych systemów alarmowych przez ZSB;

Wymagania w zakresie współpracy z SAP

- 1) MUW posiada w obiekcie system ppoż., w związku z powyższym należy skorelować planowane rozwiązania z funkcjonującymi rozwiązaniami ppoż.;
- 2) Należy zintegrować pozostałe elementy systemu z funkcjonującą w obiekcie wizualizacją sygnałów sygnalizacji pożaru;
- 3) Należy zapewnić możliwość weryfikacji stanów alarmowych ujawnianych przez SAP przy wykorzystaniu zasobów technicznych systemu (np. CCTV IP) – należy ustalić, w których miejscach kamery CCTV zostaną wykorzystane do obrazowania miejsc alarmowych (uwzględnić analizę systemu CCTV i jego dostosowanie do Systemu – zmianę rozmieszczenia lub dołożenie elementów CCTV);
- 4) System ppoż. musi współdziałać z systemami kontroli dostępu w przypadkach pożaru i ewakuacji.

Inne wymagania

- 1) Należy przewidzieć kwestie energetyczne w zakresie podtrzymania napięcia dla elementów Systemu na co najmniej 30 minut;
- 2) System Kontroli Dostępu w obiekcie MUW zaliczać się będzie do systemów dużych. System musi obsłużyć co najmniej 2000 użytkowników;
- 3) Realizacja projektu powiązana jest z ingerencją w sieć LAN MUW. Należy przewidzieć włączenie do istniejącej sieci, bądź w razie konieczności rozbudowę sieci.
- 4) Należy przewidzieć rozbudowę okablowania LAN w ramach Systemu również pod kątem CCTV IP. W etapie tym należy się dostosować do wszelkich zaleceń dotyczących projektowania i wyboru okablowania ekranowanego i nieekranowanego.
- 5) Należy uwzględnić obowiązujące normy i przepisy prawa odpowiadające planowanemu zakresowi przedsięwzięcia.
- 6) Należy oprzeć System o węzły sieci IP w budynkach MUW – w razie konieczności zaplanować zmianę lokalizacji węzłów lub ich rozbudowę, w węzłach sieci zaplanować w miarę możliwości oddzielne separowane szafy, dedykowane na potrzeby Zintegrowanego Systemu Bezpieczeństwa MUW lub zaplanować umieszczenie elementów aktywnych w części istniejących szaf rackowych;
- 7) Należy zaproponować rozwiązania pozwalające na przechowywanie zdarzeń w Systemie;
- 8) Należy zaplanować ewentualną integrację z posiadanymi przez Zamawiającego urządzeniem np. bramką detekcji materiałów metalowych.
- 9) Należy uwzględnić wymagania w zakresie dostępności dla osób niepełnosprawnych.

